

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2003-244130

(43)Date of publication of application : 29.08.2003

(51)Int.Cl.
H04L 9/14
H04L 9/32
H04M 3/56
H04M 11/00
H04N 7/15

(21)Application number : 2002-037039 (71)Applicant : CANON INC

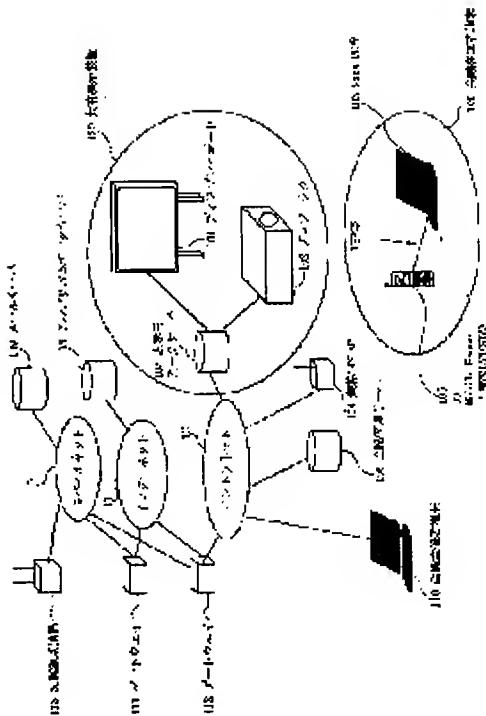
(22)Date of filing : 14.02.2002 (72)Inventor : HAMADA MASASHI

(54) CONFERENCE SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent the contents of a conference from being leaked to a third party and to securely attain conference.

SOLUTION: An authentication algorithm for using of authentication of participation terminals is dynamically changed every conferences. An encryption key to be used in a radio section between a terminal and a system is dynamically changed.



(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2003-244130

(P2003-244130A)

(43)公開日 平成15年8月29日 (2003.8.29)

(51)Int.Cl. ⁷	識別記号	F I	テマコト [*] (参考)
H 04 L 9/14		H 04 M 3/56	Z 5 C 0 6 4
	9/32	11/00	3 0 2 5 J 1 0 4
H 04 M 3/56		H 04 N 7/15	6 5 0 5 K 0 1 5
	11/00	H 04 L 9/00	6 4 1 5 K 1 0 1
H 04 N 7/15	3 0 2		6 7 5 B
	6 5 0		

審査請求 未請求 請求項の数9 OL (全10頁)

(21)出願番号	特願2002-37039(P2002-37039)	(71)出願人	000001007 キヤノン株式会社 東京都大田区下丸子3丁目30番2号
(22)出願日	平成14年2月14日 (2002.2.14)	(72)発明者	浜田 正志 東京都大田区下丸子3丁目30番2号キヤノン株式会社内
		(74)代理人	100090538 弁理士 西山 恵三 (外1名)

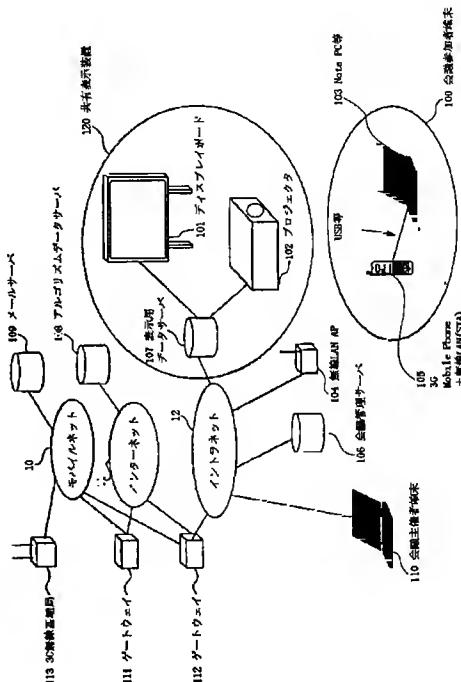
最終頁に続く

(54)【発明の名称】 会議システム

(57)【要約】

【課題】 会議内容の第3者への漏洩を防止し、安全に会議を行えるようにする。

【解決手段】 会議毎に参加端末の認証を使う認証アルゴリズムを動的に変更できるようにする。また、端末とシステム間の無線区間で使用される暗号鍵を動的に変更できるようにする。



【特許請求の範囲】

【請求項1】複数の会議参加端末を使用して会議を行う会議システムにおいて、個別もしくは単一の装置により構成され、会議に関わる管理情報を統括する会議管理サーバと、複数の認証アルゴリズムを統括管理するアルゴリズムデータサーバを有し、会議毎に、会議の開始に先立って、参加者認証のために用いる参加者認証アルゴリズムを前記会議管理サーバと前記アルゴリズムデータサーバとの間で同一化を行う手段と、前記会議参加端末に前記アルゴリズムデータサーバ上の前記同一化を行った参加者認証アルゴリズムの格納場所を通知する手段と、前記会議参加端末が当該通知された参加者認証アルゴリズムの格納場所に従って、前記アルゴリズムデータサーバにアクセスしてきた場合に、前記会議参加端末が前記参加者認証アルゴリズム入手できるようにする手段を有することを特徴とする会議システム。

【請求項2】請求項1において、

前記会議管理サーバと前記アルゴリズムデータサーバとの間で参加者認証アルゴリズムの同一化を行う手段は、会議管理サーバに格納される参加者認証アルゴリズムをアルゴリズムデータサーバへアップロード、もしくは、アルゴリズムデータサーバに格納される参加者認証アルゴリズムを会議管理サーバへダウンロードすることにより前記同一化を行うことを特徴とする会議システム。

【請求項3】請求項1において、

前記会議の開始に先立って、サーバ認証のために用いるサーバ認証アルゴリズムを前記会議参加端末と前記アルゴリズムデータサーバとの間で同一化を行う手段と、前記会議管理サーバに、前記アルゴリズムデータサーバ上のサーバ認証アルゴリズムの格納場所を通知する手段と、前記会議管理サーバが当該通知されたサーバ認証アルゴリズムの格納場所に従って、前記アルゴリズムデータサーバから前記サーバ認証アルゴリズム入手する手段を有することを特徴とする会議システム。

【請求項4】請求項3において、

前記会議参加端末と前記アルゴリズムデータサーバとの間でサーバ認証アルゴリズムの同一化を行う手段は、前記会議参加端末に格納されるサーバ認証アルゴリズムを前記アルゴリズムデータサーバへアップロード、もしくは、前記アルゴリズムデータサーバに格納されるサーバ認証アルゴリズムを前記会議参加端末へダウンロードすることにより前記同一化を行うことを特徴とする会議システム。

【請求項5】請求項1において、

前記会議参加端末に前記参加者認証アルゴリズムの格納場所を通知する手段は、前記会議管理サーバが情報を暗号化するための公開暗号化鍵も前記会議参加端末に通知

し、

前記会議参加端末が前記会議管理サーバにログインを要求する際に、当該ログイン情報上のユーザプロファイル情報を、前記公開暗号化鍵を用いて暗号化することを特徴とする会議システム。

【請求項6】請求項3において、

前記会議管理サーバにサーバ認証アルゴリズムの格納場所を通知する手段は、前記会議参加端末が情報を暗号化するための公開暗号化鍵も前記会議参加端末に通知し、前記会議管理サーバは、前記会議参加端末と前記会議管理サーバとの間の参加者認証の確認後に、前記参加者端末がネットワークに接続するためのアクセスポイントと前記会議端末との間で通信される情報の暗号化に用いる共通暗号化鍵を、前記公開暗号化鍵を用いて暗号化することを特徴とする会議システム。

【請求項7】請求項1において、

前記参加者端末は、無線を利用して前記会議システムにアクセスすることを特徴とする会議システム。

【請求項8】複数の無線端末により会議を行うための会議システムにおいて、

前記無線端末が前記会議システムにアクセスするためのアクセスポイントと、前記無線端末との無線通信で使用される暗号鍵を管理する管理手段と、前記会議システムに会議の予約が行われる毎に、前記暗号鍵の割当てを行う手段を有することを特徴とする会議システム。

【請求項9】請求項8において、

前記管理手段は、前記無線端末が前記会議システムを利用する際の認証アルゴリズムの通知も行うことを特徴とする会議システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、複数の端末による通信により会議を会議を行う会議システムに関する。

【0002】

【従来の技術】近年、プロジェクタ・大型ディスプレイ等の共有表示装置を利用したプレゼンテーションや会議が定着し、また前記共有表示装置へのアクセスを行う情報通信機器も無線通信媒体を用いるケースも増えている。

【0003】上記のような場合、共有表示装置側、情報通信機器側の双方で相互の正当性を確認する必要が生じてくる。

【0004】従来、端末相互、或いは端末データサーバ間で相互に安全に認証を行う方法として、機器内に静的に記憶している暗号化アルゴリズムを相互に指定して認証を行う方法や、認証の際に必要なパラメータを共有秘密暗号鍵で暗号化を行う方法がある。

【0005】

【発明が解決しようとする課題】しかしながら上記の従

来例では以下のような問題点があった。

【0006】第3者に対して、機器内に静的に記憶されているアルゴリズムや共有秘密暗号鍵の情報が知られないということが前提となっており、第3者に容易に傍受され得る無線通信回線を通信媒体として認証処理を行う場合、本来機密としておきたい上記静的記憶情報が、通信傍受から類推され易いという問題がある。

【0007】そこで、本発明の目的は、第3者への情報の漏洩を防止でき、安全に会議を行えるようにすることである。

【0008】

【課題を解決するための手段】本発明は上記目的を達成するために、複数の会議参加端末を使用して会議を行う会議システムにおいて、個別もしくは単一の装置により構成され、会議に関わる管理情報を統括する会議管理サーバと、複数の認証アルゴリズムを統括管理するアルゴリズムデータサーバを有し、会議毎に、会議の開始に先立って、参加者認証のために用いる参加者認証アルゴリズムを前記会議管理サーバと前記アルゴリズムデータサーバとの間で同一化を行う手段と、前記会議参加端末に前記アルゴリズムデータサーバ上の前記同一化を行った参加者認証アルゴリズムの格納場所を通知する手段と、前記会議参加端末が当該通知された参加者認証アルゴリズムの格納場所に従って、前記アルゴリズムデータサーバにアクセスしてきた場合に、前記会議参加端末が前記参加者認証アルゴリズムを入手できるようにする手段を有することを特徴とする会議システムを提供する。

【0009】また、複数の無線端末により会議を行うための会議システムにおいて、前記無線端末が前記会議システムにアクセスするためのアクセスポイントと、前記無線端末との無線通信で使用される暗号鍵を管理する管理手段と、前記会議システムに会議の予約が行われる毎に、前記暗号鍵の割当てを行う手段を有することを特徴とする会議システムを提供する。

【0010】以上の会議システムによれば、会議内容の漏洩を防止することができる。

【0011】また、参加者に成りますために必要なパラメータを安全に授受することを実現すると共に、認証に用いる認証アルゴリズム等を会議の度にダイナミックに変更することが可能となるため、同一箇所で通信傍受を続けても、類推を困難とすることが可能である。

【0012】また、会議中の通信を傍受されても、実会議情報内容の漏洩を防止できる。

【0013】

【発明の実施の形態】以下、本発明における無線通信会議システムの実施の形態について、以下に説明する。

【0014】(第一の実施例) 本発明における、無線通信会議システムの一実施例では、共有表示装置(本実施例では表示用データサーバとディスプレイボード或いはプロジェクタにより構成)と、会議参加者端末(本実施

例ではローカル無線I/F(インターフェース)を内蔵した3G(第3世代)携帯電話機とノートPC(パーソナルコンピュータ)により構成)間のローカル無線I/Fとして無線LAN(IEEE802.11b準拠システム)を通信媒体として利用する。また、会議開催情報、会議開催受領情報の授受を3G(第3世代)携帯電話網の電子メールサービスを利用し、インターネット上のサービスプロバイダのサーバ上に複数の認証アルゴリズムの維持管理を行うアルゴリズムデータサーバが存在し、前記共有表示装置とローカルネットワークで接続された会議管理サーバ、会議主催者端末と、前記3G携帯電話機(前記会議参加者端末)との間で、無線通信会議開始の際に必要となる各種情報の授受と初期認証を行う例を以下に示す。

【0015】図1が本実施例における無線通信会議システムの構成概念図である。

【0016】10は3G携帯電話網であるモバイルネットワーク、11は広域ネットワークであるインターネット、12はローカルネットワークであるイントラネット、100は無線LAN(IEEE802.11b準拠システム)を使用した無線通信を行うローカル無線I/Fを内蔵した3G携帯電話機(105)と、これに接続されるノートパソコン(103)で構成される会議参加者端末、120は表示用データサーバ(107)とこれに接続されるディスプレイボード(101)或いはプロジェクタ(102)で構成される共有表示装置、104は無線LAN(IEEE802.11b準拠システム)のアクセスポイント、106は当該無線通信会議のスケジュール、通信の際に利用するパラメータ等の管理を行う会議管理サーバ、110は会議の開催(参加者や日時、場所など)を入力する会議主催者端末、111、112はネットワーク間の接続を司るゲートウェイ、108はインターネット上のサービスプロバイダのサーバ上に存在し複数の認証アルゴリズムの維持管理を行うアルゴリズムデータサーバ、109は3G携帯電話端末への電子メールの送受を司るメールサーバ、113は3G携帯電話用の無線基地局である。なお、会議参加者端末(100)は、複数存在するものとする。

【0017】図2に本実施例における、無線LAN通信機能を内蔵した3G携帯電話端末の機能ブロック図を示す。

【0018】201は3G無線媒体の無線部、202は3G無線通信のベースバンド処理部、203は操作インターフェースであるキーパッド、204は音声データの符号化・復号化を司る音声処理部、205は3G無線通信の通信フレーム分解・組み立て部、206はワームメモリであるRAM、207は機器制御プログラムを格納するROM、208はROM207に格納されている機器制御プログラムに基づき機器制御を司る制御部、209は電池、210、211は送受話部、212は各種情報

表示部、213はユーザ情報を格納するUSIM (Universal Subscriber Identity Module)であるICカード、214は無線LAN通信媒体の無線送受信部、215は無線LANのベースバンド処理とMAC (Media Access Control)を司る機能ブロック、216は前記通信媒体経由でダウンロードしたソフトウェアを格納する不揮発メモリ、217はノートPC等の外部情報機器との通信を司る有線通信インターフェースである。

【0019】図3に前記USIMの機能構成ブロック図示す。

【0020】USIM用ICカード(213)は、3G携帯電話端末とコンタクト部(30)を介して着脱自在に接続され、端末装置側から、電源、動作用クロックの供給を受けると共に、前記端末と内蔵CPU(31)との間に通信路を形成する。

【0021】前記内蔵CPUの周辺回路は、ROM(33)、RAM(32)、EEPROM(34)、認証、暗号等の各種演算処理用のコプロセッサ(35)が存在し、これらが1チップ化されている。

【0022】図4に前記USIM内データエリアの論理ファイル構造の1実施例を示す。

【0023】本実施例ではMF (Master File、40)の直下に存在する、最上位のDF (Dedicated Files、400、410...)の1つとして無線LAN用のDF(420)が存在し、次位のDFに暗号関連DF(4200)が存在し、さらに当該DFの次位に各オペレータやマニュファクチャに対応するDF(42000)が存在し、当該DFの下に、本実施例で用いる認証アルゴリズム情報を格納するEF (Elementary File、42002)や公開暗号鍵を格納するEF(42001)を実装している。

【0024】図5に本実施例における無線LAN会議における会議立案から、無線LAN会議開始までの流れを示す。

【0025】また、図5における各フェーズでの処理を、各機器間で授受される情報シーケンスチャート(図6~8)を用いて示す。

【0026】先ず、会議主催者が会議の開催準備を行う(51、図6)場合、会議主催者端末(110)と会議管理サーバ(106)の間でリンクを形成(601)した後、会議主催者としての正当な利用者のアクセスであるかを判断する主催者レベル認証(602)処理を会議主催者端末(110)と会議管理サーバ(106)の間で行い、これに成功した後に、会議主催者端末(110)は会議主催者により入力された情報に従い、会議管理サーバ(106)に対して無線通信会議システムの利用時間、参加人数などを付加情報として会議スペースの確保要求メッセージ(603)を送信する。

【0027】前記会議管理サーバ(106)は、システムの予約状況に基づいて、当該付加情報に従った会議スペースの確保可否を会議スペース確保応答メッセージ(604)の付加情報として返送する。

【0028】会議スペースの確保が可能である旨の情報を受け取った会議主催者は、前記会議主催者端末(110)より会議への出席を依頼する出席依頼者の情報(メールアドレス、ユーザーID等の識別情報)を付加して、会議管理サーバ(106)に対して、会議出席依頼者要求メッセージ(605)を送信する。

【0029】前記会議管理サーバ(106)は、当該情報を一旦記憶すると共に、当該会議管理サーバ内に記憶されている会議参加者履歴情報との比較を行い、当該会議管理サーバ(106)が管理する前記出席依頼者の参加履歴情報を、会議出席依頼者応答メッセージ(606)に付加して前記会議主催者端末(110)へ返送する。

【0030】前記会議主催者は、当該会議参加履歴情報を前記会議主催者端末(110)上で確認し、問題がないと判断した場合、前記会議主催者端末上(110)で会議の開催を確定する操作を行うことによって、会議開催確定要求メッセージ(607)を前記会議管理サーバ(106)に対して送信する。

【0031】前記会議管理サーバ(106)は、前記会議開催確定要求メッセージ(607)を正常に受領した後、会議に関する情報の記憶が完了した旨を付加情報として会議開催確定応答(608)を返送する。

【0032】前記会議開催確定応答(608)を受け取った前記会議主催者端末(110)は、会議開催情報が正常に受け付けられた旨の表示を行った後に、会議管理サーバ(106)との間のリンクを切断する。

【0033】次に、会議管理サーバ(106)はアルゴリズムデータサーバ(108)との間でリンクを形成(610)した後、会議管理サーバとしての正当な利用者のアクセスであるかを判断するクライアント認証(611)処理をアルゴリズムデータサーバ(108)との間で行い、これに成功した後に、アルゴリズムデータサーバ(108)に対して、今回の会議における会議参加者認証のために用いる認証アルゴリズムの指定を要求するための参加者認証アルゴリズム管理要求メッセージ(612)を、当該会議への参加人数を付加情報としてアルゴリズムデータサーバ(108)に送信する。

【0034】前記参加者認証アルゴリズム管理要求メッセージ(612)を受け取った当該アルゴリズムデータサーバ(108)は、前記会議への参加人数と、自身が会議参加者として管理可能な人数とを比較し、前記会議管理サーバ(106)に対して参加者認証アルゴリズム管理応答メッセージ(613)に前記参加者認証アルゴリズムを管理することの可否情報を付加して返送する。

【0035】会議管理サーバ(106)は、前記参加者

認証アルゴリズムを管理が不可である旨の情報を受け取った場合、新たなアルゴリズムデータサーバを選択し、リンク処理(610)から新ためて行い、アルゴリズムを管理が可である旨の情報を受け取った場合は、会議参加者のプロファイル(メールアドレス、ユーザID等)を付加情報として含む会議参加者通知メッセージ(614)を前記アルゴリズムデータサーバ(108)に送信する。

【0036】アルゴリズムデータサーバ(108)は、前記会議参加者通知メッセージ(614)の正常受信の可否を、会議参加者確認メッセージ(615)で返送すると共に、正常に受信した場合は、会議参加者のプロファイル(メールアドレス、ユーザID等)を一旦記憶する。

【0037】前記会議参加者確認メッセージ(615)にて、前記会議参加者プロファイル情報が正常に前記アルゴリズムデータサーバ(108)に記憶されていないと認識した場合には、再度前記会議参加者通知メッセージ(614)の送信を再度行い、正常に記憶されたと確認された場合には、参加者認証アルゴリズムの同一化処理(616)する。

【0038】ここでの同一化処理とは、具体的には、アルゴリズムデータサーバ(108)に記憶されている認証アルゴリズムライブラリの中から、適切なものを前記アルゴリズムデータサーバ、又は前記会議管理サーバが選択し、当該会議管理サーバ(106)にダウンロードする、或いは会議管理サーバに記憶されている認証アルゴリズムライブラリの中から、適切なものを前記アルゴリズムデータサーバ、又は前記会議管理サーバが選択し、当該アルゴリズムデータサーバ(108)にアップロードすることを示している。

【0039】前記参加者認証アルゴリズムの同一化処理(616)の完了後、前記アルゴリズムデータサーバ(108)は、当該会議への参加者認証用のアルゴリズム情報にアクセスするために必要なアドレス(URL, IPアドレス等)を付加情報とする参加者認証アルゴリズム管理通知メッセージ(617)を送信する。

【0040】前記会議管理サーバ(106)は、前記参加者認証アルゴリズム管理通知メッセージ(617)の正常受信の可否を参加者認証アルゴリズム管理確認メッセージ(618)を用いて返送するこれにより、正常に受信出来なかった場合は前記会議参加者のプロファイル(メールアドレス、ユーザID等)を付加情報として含む会議参加者通知メッセージ(614)を前記アルゴリズムデータサーバ(108)に送信する手順から再度実行し、正常に受信した場合、当該会議への参加者認証用のアルゴリズム情報にアクセスするために必要なアドレス(URL, IPアドレス等)情報を記憶した後に、リンクを切断し会議準備フェーズを終了する。

【0041】次に、会議参加者に対する情報通知フェー

ズ(52、図7)の場合、会議管理サーバ(106)内で、自己宛の秘密情報を暗号化するための公開鍵暗号化方式の暗号化鍵と復号化鍵を生成し、会議関連情報として記憶した後、各会議参加者通信端末(100)に対して、会議開催通知(開催場所、開催日時、等が記載されている)メールに、前記公開鍵暗号化方式の暗号化鍵と前記会議への参加者認証用のアルゴリズム情報にアクセスするために必要なアドレス(URL, IPアドレス等)、会議の際に用いる無線LAN情報パラメータ(ESS ID(Enhanced Service Set ID)、使用予定チャネル等)を添付情報とし、メールサーバ(109)経由で送付(701、702)する。

【0042】このメールより、当該会議参加者認証用のアルゴリズム情報にアクセスするためのアドレスを入手した会議参加者端末(100)は、該アドレスを用いて前記アルゴリズムデータサーバ(108)との間で通信リンクの確立(703)し、クライアント認証(704)を終えた後、参加者認証アルゴリズムの同一化処理(705、具体的にはアルゴリズムデータサーバ(108)の該当アドレス上に記憶されている認証アルゴリズムをダウンロードする処理)を実行する。

【0043】会議参加者端末(100)は、この同一化処理により、当該アルゴリズムプログラムを前記会議参加者端末である3G携帯電話内の不揮発メモリ、或いは3GUSIM内のアルゴリズム格納エリア(物理的には34、論理的には42002)に記憶する。

【0044】また、前記記憶処理が終了した後に、アルゴリズムデータサーバ(108)との間でサーバ認証アルゴリズムの同一化処理(706)を行う。

【0045】ここでの同一化処理とは、具体的には、アルゴリズムデータサーバ(108)に記憶されている認証アルゴリズムライブラリの中から、適切なものを前記アルゴリズムデータサーバ、又は前記会議参加者端末が選択し、当該会議参加者端末にダウンロードする、或いは会議参加者端末に記憶されている認証アルゴリズムライブラリの中から、適切なものを前記アルゴリズムデータサーバ、又は前記会議参加者端末が選択し、当該アルゴリズムデータサーバ(108)にアップロードすることを示している。

【0046】前記サーバ認証アルゴリズムの同一化処理(706)の完了後、前記アルゴリズムデータサーバ(108)は、当該会議でのサーバ認証用のアルゴリズム情報にアクセスするために必要なアドレス(URL, IPアドレス等)を付加情報とするサーバ認証アルゴリズム管理通知メッセージ(707)を送信する。

【0047】前記参加端末(100)は、前記サーバ認証アルゴリズム管理通知メッセージ(707)の正常受信の可否をサーバ認証アルゴリズム管理確認メッセージ(708)を用いて返送する。なお、正常に受信出来な

かった場合は前記サーバ認証アルゴリズム同一化手順から再開し、正常に受信した場合、当該会議でのサーバ認証用のアルゴリズム情報にアクセスするために必要なアドレス（URL、IPアドレス等）情報を記憶した後に、リンクを切断する。

【0048】前記会議参加者端末（100）は、内部で、自己宛の秘密情報を暗号化するための公開鍵暗号化方式の暗号化鍵と復号化鍵を生成し、会議関連情報として記憶した後、会議管理サーバ（106）に対して、会議開催確認（会議開催通知に対する自動応答）メールに、前記公開鍵暗号化方式の暗号化鍵と前記会議でのサーバ認証用のアルゴリズム情報にアクセスするために必要なアドレス（URL、IPアドレス等）を添付情報とし、メールサーバ（109）経由で送付（710、711）する。

【0049】前記メールにより、当該会議でのサーバ認証用アルゴリズム情報にアクセスするためのアドレスを入手した会議管理サーバ（106）は、このアドレスを用いて前記アルゴリズムデータサーバ（108）との間で通信リンクの確立（712）し、クライアント認証（713）を終えた後、サーバ認証アルゴリズムの同一化処理（714、具体的にはアルゴリズムデータサーバ（108）の該当アドレス上に記憶されている認証アルゴリズムをダウンロードする処理）を実行し、同アルゴリズムを記憶した後、リンクを切断し、情報通知処理フェーズを終了する。

【0050】無線LAN会議における参加者確認フェーズ（53、図8）の場合、会議参加者端末（100）であり、無線LANステーションである携帯電話機（105）は、前記会議開催通知メール（701、702）の添付情報として通知され、記憶済みの無線LANパラメータ（ESSID、使用チャネル等）を、内部の時計情報の時刻が会議開始時刻になった時点でセットする。

【0051】無線LANアクセスポイント（104）から間欠的に送信されるビーコン（801）を検出した会議参加者端末（100）である携帯電話機（105）は、オープン認証（無線LANレベルの認証）の完了後に無線LANアクセスポイント（104）との間のリンクを確立（802）する。

【0052】前記会議参加者端末（100）は、会議管理サーバ（106）に対してログイン要求メッセージ（803）を送信する際に前記会議開催通知メール（701、702）の添付情報で通知され記憶している前記公開鍵暗号化方式の暗号化鍵を用いてユーザ名を暗号した情報を附加して送信する。

【0053】前記ログイン情報を受信した会議管理サーバ（106）は、前記公開鍵暗号化方式用の復号化鍵を用いてユーザ名を復号した後、記憶している当該会議参加者プロファイル情報と比較し、記憶してなければログイン要求を無視し、記憶していれば、前記アルゴリズム

データサーバ（108）との間で同一化を行った参加者認証アルゴリズムにおいて用いるための鍵情報を附加した参加者認証要求メッセージ（804）を前記会議参加者端末（100）に送信すると共に、この鍵を用いた参加者認証アルゴリズム演算の結果を算出する。

【0054】前記会議参加者端末（100）は、アルゴリズムデータサーバ（108）よりダウンロードした参加者認証アルゴリズムと、前記参加者認証要求メッセージ（804）にて通知された鍵を用いて演算を行い（805）、この結果を参加者認証応答メッセージ（806）に付加して会議管理サーバ（106）に返送する。

【0055】前記会議管理サーバ（106）は、前記自己内部での参加者認証アルゴリズム演算の結果と、前記参加者認証応答メッセージ（806）に付加して送付された前記会議参加者端末（100）での演算結果を比較し、一致しなければ認証失敗と見なし、会議管理サーバ側のトリガでリンクを切断し、一致すれば、参加者認証が確認（807）されたと認識し、会議開催確認メール（710、711）に添付して通知し、会議参加者毎に記憶している前記公開鍵暗号化方式の暗号化鍵から、当該参加者に対応する暗号化鍵を用いて、無線LAN区間の通信フレーム上データの暗号化に用いる共通鍵暗号化方式の秘密鍵（WEP（Wired Equivalent Privacy）鍵）や共有表示装置（120）を構成する表示用データサーバ（107）にアクセスするためのLANアドレス情報、ログインID、パスワード等の情報を、前記公開鍵を用いてを暗号化し、ログイン応答メッセージ（808）に付加して会議参加者端末（100）に返送すると共に、共有表示装置（120）内の表示用データサーバ（107）との間で通信リンクを確立（809）し、前記表示用データサーバに対してクライアント認証（810）を行った後に、共有表示装置（120）を統括する表示用データサーバ（107）に対して、会議参加予定者が前記無線LAN通信環境にログインした旨を通知するために前記会議参加者端末ユーザー名、アドレス情報等を附加した会議出席者通知メッセージ（811）を送信する。

【0056】前記表示用データサーバ（107）は、会議管理サーバ（106）から会議出席者通知メッセージ（811）により通知された前記会議参加者端末ユーザー名、アドレス情報を記憶し、当該無線LAN会議における参加者端末の表示用データサーバへのアクセスを許可（813）すると共に、会議管理サーバ（106）にその旨を報告する目的で会議出席者確認メッセージ（812）を返送した後、通信リンク（814）を切断する。

【0057】また、前記参加者端末（100）は、前記ログイン応答メッセージ（808）の受領後、必要に応じて、前記アルゴリズムデータサーバ（108）との間で同一化を行った参加者認証アルゴリズムにおいて用いるための鍵情報を附加したサーバ認証要求メッセージ

(815)を前記会議管理サーバ(106)に送信すると共に、この鍵を用いた参加者認証アルゴリズム演算の結果を算出する。

【0058】前記会議管理サーバ(106)は、アルゴリズムデータサーバ(108)よりダウンロードしたサーバ認証アルゴリズムと、前記サーバ認証要求メッセージ(815)にて通知された鍵を用いて演算を行い(816)、この結果をサーバ認証応答メッセージ(817)に付加して会議参加者端末(817)に返送する。

【0059】前記会議参加端末(100)は、前記自己内部でのサーバ認証アルゴリズム演算の結果と、前記サーバ認証応答メッセージ(817)に付加して送付された前記会議管理サーバ(106)での演算結果を比較し、一致しなければ認証失敗と見なし、会議参加者端末側のトリガでリンクを切断し、一致すれば、サーバ認証が確認(818)されたと認識し、共有表示装置(120)の制御を司る表示用データサーバ(107)にログインし無線LANを通信媒体としたネットワーク会議への参加(819)を開始する。

【0060】以上の無線通信会議(無線LANを用いたネットワーク会議)参加までの処理により、前記無線通信会議に用いる無線通信媒体(無線LAN媒体)を傍受していても、実会議情報内容を傍受することが困難になると共に、参加者に成りますために必要なパラメータを安全に授受することを実現し、認証に用いる認証アルゴリズム等を会議の度にダイナミックに変更することが可能となるため、同一箇所で通信傍受を続けても、類推を困難とすることが可能となる。

【0061】(他の実施例)第一の実施例では、会議参加者の所持する無線通信端末の構成を、3G携帯電話と無線LANの組み合わせの例を示したが、他の複数の通信媒体との組み合わせ、例えば、有線LANと無線LAN、2G携帯電話(PDC、GSM等)と無線LANとの組み合わせ、等を用いても同様の効果が得られる。

【0062】また、会議管理サーバ、表示用データサーバ、アルゴリズムデータサーバのように、各機能ごとに物理的に独立したサーバを構築する例を示したが、物理的に同一サーバ上に構築しても同様の効果が得られる。

【0063】

【発明の効果】以上説明したように、本発明によれば、会議内容の漏洩を防止することができる。

【0064】また、参加者に成りますために必要なパ

ラメータを安全に授受することを実現すると共に、認証に用いる認証アルゴリズム等を会議の度にダイナミックに変更することが可能となるため、同一箇所で通信傍受を続けても、類推を困難とすることが可能である。

【0065】また、会議中の通信を傍受されても、実会議情報内容の漏洩を防止できる。

【図面の簡単な説明】

【図1】本実施例における無線通信会議システムの構成図

【図2】本実施例における3G携帯電話、無線LAN、共用端末の機能ブロック図

【図3】本実施例における3G携帯電話用USIMの機能ブロック図

【図4】本実施例における3G携帯電話用USIMファイル論理構造図

【図5】本実施例における無線LAN会議立案から開始までのフロー

【図6】本実施例における無線LAN会議開催準備フェーズのシーケンスチャート

【図7】本実施例における無線LAN会議開催情報通知フェーズのシーケンスチャート

【図8】本実施例における無線LAN会議開始前の参加者認証フェーズのシーケンスチャート

【符号の説明】

10 広域モバイルネットワーク

11 インターネット

12 イントラネット

100 会議参加者端末

101 ディスプレイボード

102 プロジェクタ

103 ノートPC

104 無線LANアクセスポイント

105 無線LANステーション機能内蔵3G携帯電話機

106 会議管理サーバ

107 表示用管理サーバ

108 認証アルゴリズム管理サーバ

109 メールサーバ

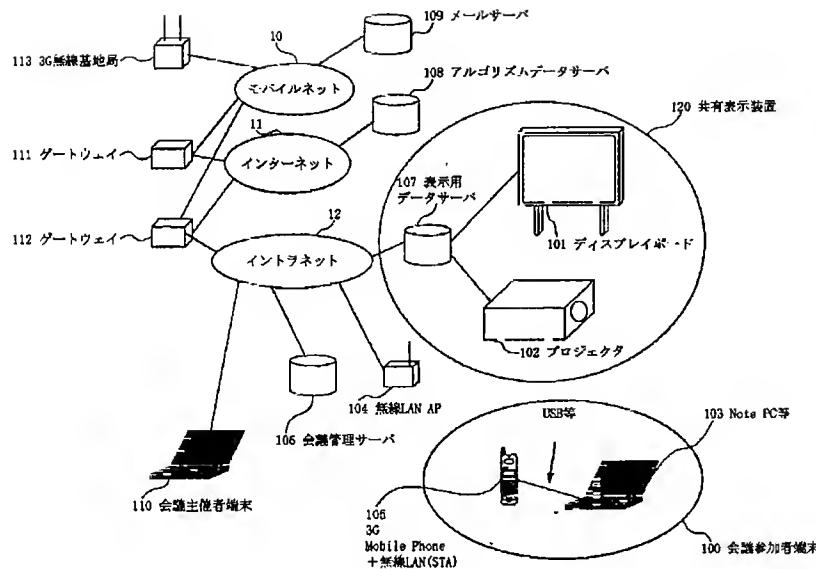
110 会議主催者端末

111 モバイルネットゲートウェイ

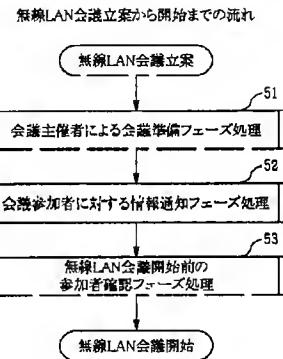
112 イントラネットゲートウェイ

113 3G無線基地局

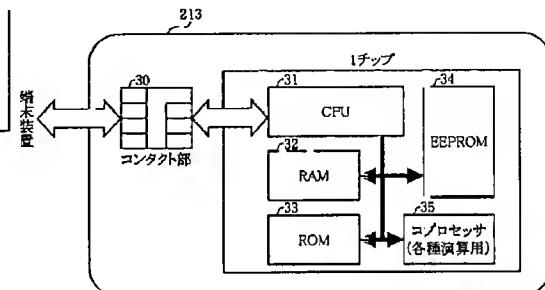
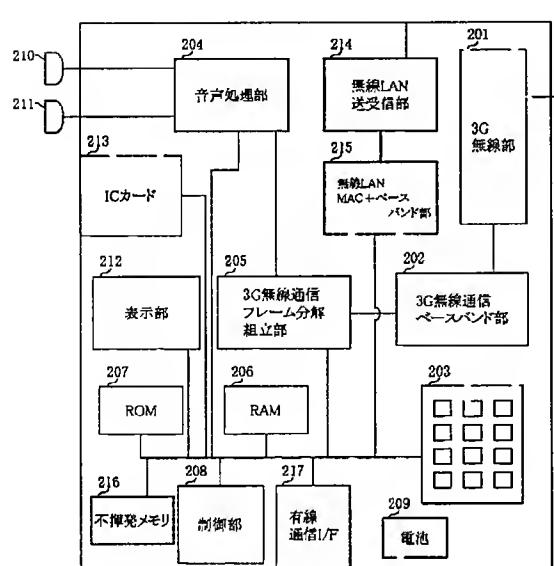
【図1】



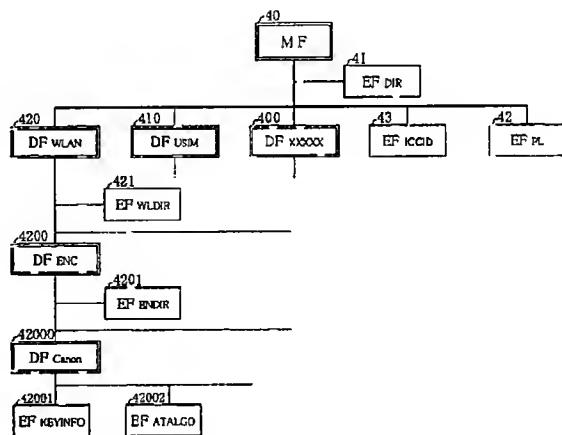
【図5】



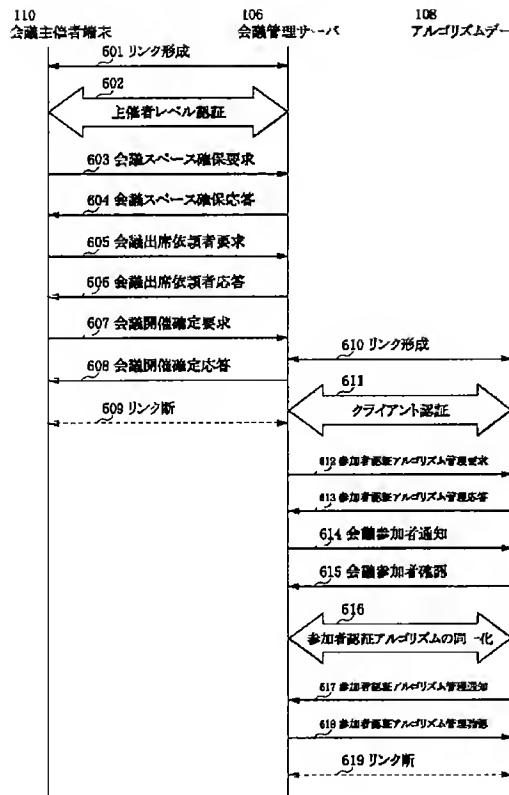
【図2】



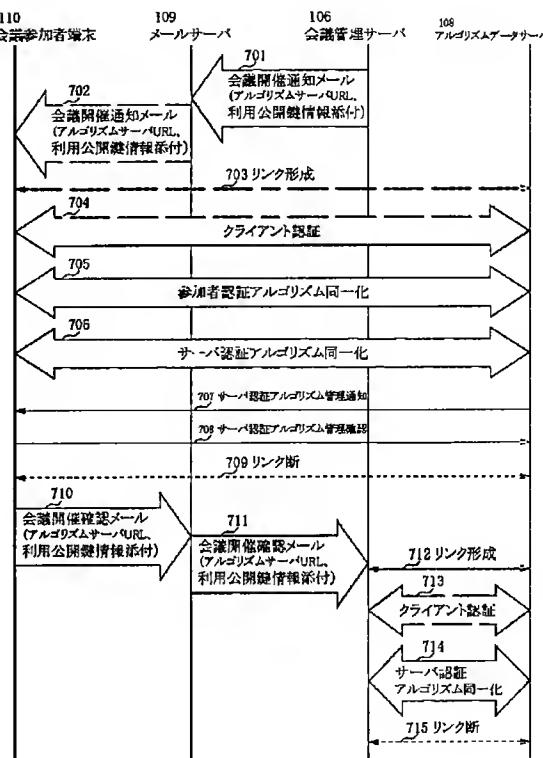
【図3】



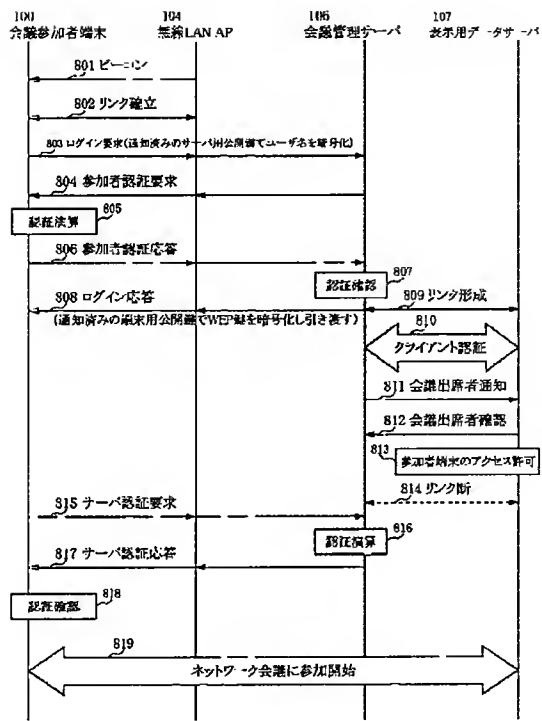
【図6】



【図7】



【図8】



フロントページの続き

Fターム(参考) 5C064 AA02 AC01 AC12 AC20 AC22
AD06
5J104 AA07 AA16 EA04 KA04 PA07
5K015 AA12 AD01 AD02 AD05 AF06
JA01
5K101 KK07 NN03 NN14 NN18 NN25
PP04 TT02 UU18